

ЗАТВЕРДЖЕНО
ЄААД.468244.185-ЛУ

Підп. та дата	
Інв. № дубл	
Взам. інв. №	
Підп. та дата	
Інв. № ориг.	

Центр сертифікації ключів ринку електричної енергії

Комплексна система захисту інформації

Політика безпеки інформації

ЄААД.468244.185.Д2.01

2014 р.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ	3
ТЕРМІНИ ТА ВИЗНАЧЕННЯ.....	4
1 ЗАГАЛЬНІ ПОЛОЖЕННЯ.....	5
2 ПРИЗНАЧЕННЯ І СТРУКТУРА ДОКУМЕНТА.....	6
3 МЕТА ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЇ В ЦСК.....	7
4 ОПИС КОМПОНЕНТІВ ЦСК ТА ТЕХНОЛОГІЇ ОБРОБКИ ІНФОРМАЦІЇ.....	8
5 ОПИС ОСНОВНИХ ЗАГРОЗ ДЛЯ ЦСК	10
6 ВИМОГИ ДО ЗАХИСТУ ВІД ЗАГРОЗ	11
7 ПРИНЦИПИ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЇ	13
8 ОПИС ПРАВИЛ РОЗМЕЖУВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ	14
9 ОПИС ПРАВИЛ МАРКУВАННЯ НОСІЇВ ІНФОРМАЦІЇ.....	15
10 ОПИС ОСНОВНИХ АТРИБУТІВ ДОСТУПУ	16
11 ОПИС ПРАВИЛ РОЗМЕЖУВАННЯ ДОСТУПУ	17
12 ПРАВИЛА АДМІНІСТРУВАННЯ КЗЗ І РЕЄСТРАЦІЇ ДІЙ КОРИСТУВАЧІВ	20
13 ЗАГАЛЬНІ ПРАВИЛА ВИКОРИСТОВУВАННЯ КРИПТОГРАФІЧНИХ ЗАСОБІВ	22
14 ПОРЯДОК ПРОВЕДЕННЯ РОБІТ ПО ЗАБЕЗПЕЧЕННЮ ФУНКЦІОНУВАННЯ.....	23
15 ВІДПОВІДАЛЬНІСТЬ ЗА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В ЦСК	24
16 ПОРЯДОК РОЗРОБКИ І СУПРОВОДУ КСЗІ	26
17 ПОРЯДОК РЕАГУВАННЯ НА ПОРУШЕННЯ БЕЗПЕКИ	27
18 ОРГАНІЗАЦІЯ НАВЧАННЯ І ПЕРЕПІДГОТОВКИ ПЕРСОНАЛУ.....	28

ПЕРЕЛІК СКОРОЧЕНЬ

БД	- База даних
ДСТУ	- Державний стандарт України
ЕЦП	- Електронний цифровий підпис
ІзОД	- Інформація з обмеженим доступом
КЗЗ	- Комплекс засобів захисту
КСЗІ	- Комплексна система захисту інформації
НД	- Нормативний документ
ОС	- Операційна система
ПЗ	- Програмне забезпечення
ПРД	- Правила розмежування доступу (користувачів до об'єктів захисту)
ПТК	- Програмно-технічний комплекс
ТЗІ	- Технічний захист інформації
ЦСК	- Центр сертифікації ключів

ТЕРМІНИ ТА ВИЗНАЧЕННЯ

У цьому документі використовуються терміни та визначення згідно з:

- ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення;
- НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1 Створюваний ЦСК є інформаційно-телекомунікаційною системою. Згідно Законів України “Про інформацію”, “Про захист інформації в інформаційно-телекомунікаційних системах”, а також НД ТЗІ 1.4-001-2000 в ЦСК підлягає розробці і створенню КСЗІ.

1.2 Порядок розробки і створення КСЗІ в ЦСК регламентується комплексом нормативно-правових документів в області технічного і криптографічного захисту інформації, перелік яких визначений Адміністрацією Держспецзв'язку України.

1.3. Інформаційні ресурси ЦСК є певною цінністю, мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю загроз, які можуть привести до зниження цінності інформаційних ресурсів. Забезпечення безпеки інформації в такій системі вимагає проведення цілого комплексу заходів відповідно розробленій політиці безпеки інформації.

1.4. Під інформаційною безпекою розуміється захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних дій природного або штучного характеру, які можуть завдати збитку власникам або користувачам інформації і підтримуючій інфраструктурі.

1.5. Політика безпеки інформації в ЦСК регламентує порядок обробки інформації і спрямована на забезпечення захисту інформації, оброблюваної в ЦСК і його складових частинах, і прав власника ЦСК від загроз.

1.6 Нормативно-правовою базою створення політики безпеки інформації в ЦСК є наступні документи:

- Закон України “Про інформацію”;
- Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”;
- Закон України „Про електронний цифровий підпис”;
- Кодекс законів про працю України (КЗпП);
- Концепція технічного захисту інформації в Україні. Затверджена постановою Кабінету Міністрів України від 08.10.97 р. № 1126;
- Положення про технічний захист інформації в Україні. Затверджене Указом Президента України від 27.09.99 р. №1229;
- НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБ України від 28.04.99 р. № 22;
- НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБ України від 28.04.99 р. № 22;
- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБ України від 28.04.99 р. № 22;
- НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБ України від 28.04.99 р. № 22;
- НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення системи захисту інформації в автоматизованій системі. Затверджений наказом ДСТСЗІ СБ України від 28.04.99. р. № 22;
- НД ТЗІ 1.4-001-2000 Положення про службу захисту інформації в автоматизованій системі. Затверджений наказом ДСТСЗІ Служби безпеки України від 04.12.2000 р. № 53;
- Правила посиленої сертифікації. Затверджені наказом ДСТСЗІ СБ України № 50 від 10.05.2006 р.

2 ПРИЗНАЧЕННЯ І СТРУКТУРА ДОКУМЕНТА

2.1 Даний документ призначений для керівного складу ЦСК та співробітників ЦСК.

2.2 В цьому документі приведені основні (базові) положення політики безпеки інформації в ЦСК, які представлені у вигляді структурованої сукупності документованих управлінських рішень (правил) керівництва ЦСК, спрямованих на захист інформації і асоційованих з нею ресурсів. Положення даного документа є основними при формуванні і конкретизації політик безпеки інформації для окремих складових частин і інформаційних (функціональних) підсистем ЦСК, послуг, компонентів тощо, шляхом їх подальшого уточнення і конкретизації.

3 МЕТА ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЇ В ЦСК

3.1 Метою політики безпеки інформації в ЦСК є попередження або зниження можливостей реалізації загроз і мінімізації збитку власнику і користувачам ЦСК до допустимого рівня в процесі обробки інформації у функціональних підсистемах ЦСК шляхом комплексного використання організаційних (адміністративних) заходів, правових, морально-етичних норм, фізичних і технічних (апаратних і програмних) способів і засобів захисту інформації.

3.2 Об'єктами захисту є: критична інформація, інформація з обмеженим доступом, ресурси ЦСК, права власників оброблюваної інформації і власника ЦСК, права користувачів.

4 ОПИС КОМПОНЕНТІВ ЦСК ТА ТЕХНОЛОГІЇ ОБРОБКИ ІНФОРМАЦІЇ

4.1 Організаційно-топологічна структура ЦСК

Функціональну структуру ЦСК утворюють функції, задачі й інформаційні зв'язки програмно-технічних комплексів спеціалізованих інформаційних підсистем ЦСК, що взаємодіють між собою, а також інформаційних підсистем віддалених користувачів.

ЦСК вирішує наступні цільові задачі:

обслуговуванням сертифікатів користувачів, що включає:

- реєстрацію користувачів;
- сертифікацію відкритих ключів користувачів;
- розповсюдження сертифікатів;
- управління статусом сертифікатів та розповсюдження інформації про статус сертифікатів;
- надання послуг фіксування часу;

надання користувачам:

- засобів ЕЦП та шифрування даних;
- засобів генерації особистих і відкритих ключів.

Структура та склад обчислювальної системи, програмного та програмно-апаратного забезпечення визначається особливостями ПТК ЦСК, що використовується у складі ЦСК. Обчислювальна система ПТК ЦСК повинна відповідати вимогам, що містяться в правилах посиленої сертифікації.

До складу ПТК ЦСК входять такі технічні засоби:

- РС адміністратора безпеки;
- РС адміністратора сертифікації та системного адміністратора;
- РС адміністратора реєстрації;
- центральні сервери ЦСК;
- сервери взаємодії;
- сервер моніторингу та синхронізації часу;
- комунікаційне обладнання (комутатори ЛОМ, комутатор РС, МЕ);
- РС генерації ключів користувачів.

ЦСК складається з наступних логічно відокремлених сегментів, які взаємодіють по відкритим каналам зв'язку:

- серверний сегмент у складі:
 - центральні сервери ЦСК;
 - сервери взаємодії;
 - сервер моніторингу та синхронізації часу;
 - комунікаційне обладнання (комутатори ЛОМ, комутатор РС, МЕ);
- РС персоналу у складі:
 - РС адміністратора безпеки;
 - РС адміністратора сертифікації та системного адміністратора;
 - РС адміністратора реєстрації;
 - РС генерації ключів користувачів.

4.2 Система зв'язку та обміну даними

Обмін даними у формі повідомлень між сервером взаємодії та засобами передачі даних віддалених користувачів та персоналу ЦСК забезпечується комплексом комунікаційних програм (HTTP-сервера, LDAP-сервера, поштового сервера тощо). При віддаленому доступі до сервера взаємодії в якості мережевого протоколу використовується протокол TCP/IP.

4.3 Категорії користувачів ЦСК

У ЦСК передбачені наступні категорії користувачів:

- віддалений користувач ЦСК, яким може бути користувач, взаємодія якого з ЦСК можлива лише за умов обміну даними через сервер взаємодії;
- адміністратор реєстрації ЦСК яким є користувач ЦСК, відповідальний за отримання від абонентів заявок на формування, скасування, блокування та поновлення сертифікатів ключів;

- адміністратор безпеки ЦСК, яким є адміністратор, відповідальний за дотриманням політики безпеки в ЦСК;
- системний адміністратор ЦСК, яким є адміністратор, відповідальний за організацію експлуатації та технічного обслуговування програмно-технічного комплексу центру, а також відповідальний за формування сертифікатів абонента, списків відкликаних сертифікатів та позначок часу.

Склад персоналу забезпечує цілодобову експлуатацію ЦСК і визначається штатним розкладом.

Основні вимоги до адміністраторів ЦСК:

- вища освіта по профілям: інформаційна безпека, обчислювальна техніка, програмування;
- проходження курсу спеціальної підготовки по профілю діяльності;
- проходження стажування на ЦСК.

4.4 Організаційно-технічна структура ЦСК

Організаційно-технічна структура ЦСК являє собою локалізований, багатомашинний та багатокористувацький комплекс з відокремленими робочими станціями та серверами, у якому оброблюється інформація різних категорій і існує необхідність її передачі через незахищене середовище.

Згідно НД ТЗІ 2.5-005-99 ЦСК і його складові частини класифікуються наступним чином:

- ЦСК в цілому відноситься до 3 класу - підклас 3. КЦД;
- серверний сегмент ЦСК, РС адміністраторів відноситься до 2 класу - підклас 2.КЦД;
- робоча станція генерації ключів користувачів до 1 класу - підклас 1.КЦД.

5 ОПИС ОСНОВНИХ ЗАГРОЗ ДЛЯ ЦСК

5.1 Опис основних загроз для ЦСК наведено в окремому документі “Модель загроз безпеки інформації”.

6 ВИМОГИ ДО ЗАХИСТУ ВІД ЗАГРОЗ

6.1 Захист критичної інформації і ресурсів повинен забезпечуватися на всіх технологічних етапах обробки і всіх режимах функціонування ЦСК.

6.2 Захист інформації повинен забезпечуватися від моменту створення об'єкту обчислювальної системи або його імпорту в систему і аж до його знищення або експорту з системи. Всі запити на доступ до об'єкту і об'єкту на доступ до інших об'єктів повинні контролюватися КЗЗ.

6.3 Для реалізації політики безпеки КЗЗ повинен забезпечити ізоляцію об'єктів усередині сфери управління КСЗІ і гарантувати розмежування запитів доступу і управління потоками інформації між об'єктами. Для цього кожний об'єкт повинен мати певний набір атрибутів доступу, які включають унікальний ідентифікатор і іншу інформацію, дозволяючи перевіряти легальність запитів доступу і визначати його права доступу і/або права доступу до нього.

6.4 Для реалізації політики безпеки КЗЗ повинен забезпечити ізоляцію об'єктів мережі ЦСК і гарантувати розмежування запитів доступу і управління потоками інформації між об'єктами ЦСК. Для цього для кожного об'єкту ЦСК складаються списки доступу, які визначають права доступу інших об'єктів мережі до нього. Права доступу повинні надаватися у мінімально необхідному для функціонування ЦСК об'ємі. У всіх складових частинах ЦСК повинна забезпечуватися цілісність і доступність всіх об'єктів захисту. Додатково, в процесі функціонування мережі ЦСК повинна забезпечуватися конфіденційність інформації з обмеженим доступом (ІЗОД).

6.5 КЗЗ повинні забезпечувати адміністративне управління доступом за допомогою паролів і призначеного для користувача імені (унікального ідентифікатора).

6.6 Паролі користувачів повинні мати довжину не менше 8 символів і зберігатися в зашифрованому вигляді в області пам'яті, що недоступна користувачу. Пароль користувача, його довжина і термін дії призначаються адміністратором безпеки ЦСК.

6.7 Час і дні тижня, коли користувач має право входити в систему, призначається адміністратором безпеки ЦСК. Користувачу не повинен надаватися доступ при спробі входу в систему в будь-який інший час. Спроби доступу повинні реєструватися в системному журналі безпеки.

6.8 Комплекси засобів захисту повинні забезпечувати реєстрацію призначеного для користувача імені, дати і часу останнього входу/виходу в(з) систему(и).

6.9 Комплекси засобів захисту повинні забезпечувати реєстрацію спроб несанкціонованого доступу і блокування системи або клавіатури після певної кількості спроб. Число спроб призначається адміністратором безпеки ЦСК.

6.10 Для забезпечення безпеки інформації під час її обробки в ЦСК створюється КСЗІ, яка представляє собою сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ЦСК.

6.11 КСЗІ в ЦСК повинні забезпечувати функціональні послуги захисту (послуги безпеки) і послуги спостереженості.

6.12 Вимоги до захисту конфіденційної інформації і архітектура КСЗІ ЦСК визначаються службою захисту інформації ЦСК і затверджуються керівництвом ЦСК у відповідності з вимогам законодавчих і інших нормативних документів України.

6.13 Операційні системи і СУБД, які використовуються в інформаційних мережах ЦСК, повинні містити інтегровану систему захисту інформації, основним призначенням якої є контроль і управління доступом до об'єктів системи. Інтеграція системи захисту інформації означає, що вона впливає на всю операційну систему. Компоненти системи захисту інформації, які виконуються в призначеному і привілейованому для користувача режимах, повинні гарантувати, що локальні ресурси і ресурси ЦСК не можуть використовуватися без відповідного дозволу.

6.14 Криптографічний захист конфіденційної інформації при передачі у каналах зв'язку доцільно здійснювати на прикладному (сеансовому), мережевому і/або каналному рівнях з використанням механізмів симетричного і асиметричного шифрування, формування електронного цифрового підпису і автентифікації.

6.15 КСЗІ ЦСК повинна забезпечувати виконання таких основних функцій:

- контроль входу (реєстрації) користувачів в систему;
- ідентифікація і автентифікація користувачів при доступі в систему;
- реєстрація спроб безпосереднього доступу користувача до об'єктів системи і непрямого доступу (зробленого процесом, який виконується на користь користувача);

- контроль коректності доступу користувачів до об'єктів системи;
- спостереження і управління доступом користувачів до об'єктів (типу файлів, каталогів, принтерів та ін.);
- визначення прав і способу доступу залежно від типу об'єкту системи;
- створення, редагування і збереження облікової інформації про користувачів, групи користувачів і об'єкти;
- спостереження і реєстрацію як системних подій (використання системи або індивідуальних додатків), так і подій, пов'язаних з безпекою системи;
- сигналізація (сповіщення) про спроби порушення захисту;
- контроль виконання встановленої політики безпеки;
- аналіз і уточнення політики безпеки;
- контроль цілісності локального і мережного програмного забезпечення (включаючи програмне забезпечення КЗЗ);
- контроль цілісності конфігурації інформаційних мереж ЦСК;
- захист від вірусів;
- управління логічною структурою інформаційних мереж ЦСК.

6.16 До складу ЦСК входять РС та сервери, які взаємодіють тільки в межах необхідних для функціонування ЦСК.

6.17 Віддалений доступ користувачів повинен здійснюватися тільки до серверу взаємодії, до усіх інших складових ЦСК віддалений доступ заборонений.

6.18 Міжмережний екран ЦСК повинен реалізувати такі основні функції:

- фільтрацію мережевого трафіку між зовнішніми телекомунікаційними мережами та серверами взаємодії;
- виявлення та блокування атак спрямованих на сервер взаємодії та на ЛОМ серверного сегменту ЦСК.

6.19 Адміністратор безпеки ЦСК має статус “власника” всього функціонального (прикладного, спеціального і системного) програмного забезпечення і ресурсів (файлів, принтерів тощо) на всіх РС та серверах ЦСК. На адміністратора безпеки ЦСК покладається виконання таких категорій функцій:

- адміністрування облікових записів користувачів і груп;
- адміністрування та моніторинг безпеки на робочих станціях та серверах ЦСК;
- адміністрування та моніторинг подій і ресурсів мережі;
- адміністрування та моніторинг міжмережного екрану та каналів зв'язку;
- адміністрування та моніторинг резервного копіювання і відновлення даних.

6.20 Адміністратор безпеки ЦСК повинен контролювати всі події, які пов'язані з безпекою, оперативно коректувати список контрольованих подій безпеки, переглядати, видавати на принтер і/або заносити в архів. Доступ до цих контрольних даних повинен бути обмежений.

6.21 Параметри робочого середовища будь-якого технічного засобу ЦСК повинні визначатися профілем користувача. Кожному обліковому запису користувача повинен відповідати його профіль.

6.22 Адміністратор безпеки ЦСК на основі профілю користувача повинен мати нагоду обмежити доступ користувача до додатків і параметрів середовища оточення.

6.23 Управління привілеями і правами доступу користувачів (груп) до мережних і локальних ресурсів ЦСК повинне здійснюватися тільки адміністратором безпеки з РС адміністратора безпеки або локально.

7 ПРИНЦИПИ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЇ

7.1 Відповідно призначення ЦСК виділяються такі групи користувачів в цілому:

- користувачі зі складу обслуговуючого персоналу, які забезпечують роботу складових частин ЦСК;
- користувачі зі складу технічного обслуговуючого персоналу ЦСК;
- користувачі, які використовують інформацію ЦСК;

Для груп користувачів необхідно підтримувати такі основні рівні повноважень:

- вищого керівництва, яке має право перевести систему захисту інформації ЦСК в режим з'ясування арбітражних ситуацій;
- адміністратора безпеки;
- системного адміністратора;
- інших адміністраторів та операторів.

7.2 У ЦСК повинно бути реалізоване адміністративне управління доступом. Користувачі не повинні мати права змінювати атрибути доступу.

7.3 Всі спроби будь-якого суб'єкта отримати доступ до будь-якого об'єкту інформаційної мережі ЦСК повинні оброблятися монітором безпеки, який повинен порівнювати інформацію безпеки суб'єкта-користувача з інформацією безпеки списку контролю доступу об'єкту і дозволяти або забороняти доступ відповідно політиці безпеки.

7.4. Дозволи користувачам на виконання будь-яких дій з мережними і локальними ресурсами ЦСК повинні регулюватися привілеями і правами доступу. Привілеї регулюють права користувача на виконання системних операцій. Права доступу визначають правомірність виконання користувачем (групою користувачів) конкретних дій з ресурсами (файлами, принтерами тощо).

7.5 Права доступу до загальних ресурсів повинні діяти лише при підключенні користувачів до ресурсів будь-якого технічного засобу по мережі і ніяк не обмежувати локальний доступ до загального ресурсу, розташованого локально.

7.6 Управління привілеями і правами доступу користувачів (груп) до мережних і локальних ресурсів ЦСК повинне здійснюватися централізовано тільки адміністратором безпеки з РС адміністратора безпеки або локально.

7.7 На всіх робочих станціях ЦСК дозвіл користувачам (групам) на доступ до ресурсів (папок, файлів, принтерів і т.п.) повинен визначатися виконуваними службовими обов'язками і надаватися в мінімально необхідному об'ємі.

7.8 Всі користувачі робочих станцій повинні мати право запускати виконувані коди функціональних задач своїх АРМ, але не змінювати їх.

7.9 Дозволи на мережний доступ користувачів до серверу ЦСК повинні надаватися тільки до даних, що спільно використовуються.

7.10 Для надання однакових прав і привілеїв доступу до ресурсів серверу ЦСК відразу декільком користувачам останні повинні бути організаційно з'єднані в локальні групи. Користувач може бути членом декількох груп одночасно.

8 ОПИС ПРАВИЛ РОЗМЕЖУВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ

8.1 Об'єктами даних правил є інформаційні потоки:

- внутрішні (між активними і пасивними об'єктами усередині однієї ПЕОМ);
- локальні (обмін між робочими станціями і серверами);
- міжмережні (віддаленого) обміну з користувачами і споживачами мережі ЦСК.

8.2 Локальні і міжмережні інформаційні потоки, які містять інформацію з обмеженим доступом, повинні бути відокремлені від інформаційних потоків з відкритою інформацією.

8.3 У свою чергу, локальні і міжмережні інформаційні потоки з ІзОД повинні бути відокремлені від інформаційних потоків оперативно-службової інформації.

8.4 Розмежування повинно здійснюватися на прикладному рівні шляхом застосування різних ідентифікаторів безпеки, мережних портів, особистих ключів автентифікації тощо.

8.5 Вихідний/вхідний міжмережний обмін з віддаленими користувачами повинен здійснюватися тільки через сервер взаємодії та міжмережний екран.

8.6 Вихідні інформаційні потоки від серверів ЦСК на передачу віддаленому користувачу повинні проходити тільки через сервер взаємодії та міжмережний екран. Віддалені користувачі не повинні мати безпосереднього (прямого) доступу на сервери ЦСК.

8.7 Запуск процесів вхідного міжмережного обміну з віддаленими користувачами повинен здійснюватися з технічних засобів користувачів ЦСК, права яких визначені регламентом ЦСК.

9 ОПИС ПРАВИЛ МАРКУВАННЯ НОСІЇВ ІНФОРМАЦІЇ

9.1 Всі роботи, пов'язані з рішенням на робочих станціях та серверах ЦСК задач службового характеру з використанням інформації з обмеженим доступом, і видача результатів повинні проводитися тільки з використанням врахованих в установленому порядку носіїв інформації (магнітні дискети, диски та електронні носії інформації тощо).

9.2 Магнітні дискети, диски та електронні носії інформації, що не містять конфіденційної інформації, повинні враховуватися в звичайному порядку.

9.3 При роботі на РС та серверах ЦСК користувач несе персональну відповідальність за дотримання встановленої адміністратором безпеки політики безпеки (включаючи визначення необхідності копіювання (знищення) конфіденційної інформації, правильність визначення грифа конфіденційності вхідних та вихідних даних, носіїв інформації тощо), а також ведення журналу обліку роботи.

10 ОПИС ОСНОВНИХ АТРИБУТІВ ДОСТУПУ

10.1 Ідентифікаційне ім'я і пароль користувача в системі вводяться в дію, модифікуються і відміняються адміністратором безпеки.

10.2 Пароль кожного користувача повинен мати такі атрибути: мінімально допустима довжина пароля; максимальний і мінімальний терміни дії пароля; унікальність пароля; параметри блокування облікового запису; параметри роботи з паролем.

10.3 Ідентифікатор безпеки користувача або групи користувачів ЦСК повинен бути унікальний в часі і в просторі, тобто існування двох однакових ідентифікаторів безпеки повинне бути виключено.

10.4 При створенні нового облікового запису системи захисту інформації, ОС повинна автоматично генерувати новий унікальний ідентифікатор, який повинен застосовуватися як ідентифікатор облікового запису користувача в об'єкті-користувачі і списках контролю доступу.

10.5 Ідентифікатор облікового запису користувача не повинен залежати від його ідентифікаційного імені.

10.6 При знищенні облікового запису з яким-небудь ім'ям користувача і наступним створенням нового облікового запису з тим же ідентифікаційним ім'ям йому повинен бути привласнений новий ідентифікатор без відновлення прав доступу до ресурсів, як раніше.

10.7 Об'єкт-користувач повинен містити ідентифікатори безпеки користувача, ідентифікатори безпеки груп, до складу яких він входить, і привласнені права доступу і привілею.

10.8 Всі об'єкти захисту повинні описуватися такими основними атрибутами безпеки:

- ідентифікатор безпеки власника, який вказує на користувача або групу, яка є власником об'єкту захисту інформаційної мережі ЦСК;
- ідентифікатор безпеки групи;
- список управління доступом, який повинен містити права користувачів і груп на доступ до об'єкту. Список повинен складатися з окремих записів контролю доступу, кожний з яких включає маску доступу, яка визначає можливі дії користувача або групи для конкретного типу об'єкту захисту. Дозволи повинні надаватися на основі цієї маски доступу. Список управління доступом повинен задаватися адміністратором безпеки.

10.9 В облікових записах користувачів повинні міститися такі відомості:

- ім'я користувача;
- пароль доступу;
- правила модифікації пароля;
- профіль користувача;
- дозволений час роботи (дні і години);
- термін дії запису.

11 ОПИС ПРАВИЛ РОЗМЕЖУВАННЯ ДОСТУПУ

11.1 Для реєстрації в системі кожний користувач повинен мати ідентифікаційне ім'я і пароль, які призначаються, модифікуються і відміняються адміністратором безпеки.

11.2 Користувачі не повинні мати права змінювати ідентифікаційне ім'я, значення і термін дії пароля, який встановлений адміністратором безпеки ЦСК.

11.3 Користувачі або групи користувачів ЦСК повинні ідентифікуватися в системі за допомогою унікального ідентифікатора безпеки (SID). Користувачі не повинні мати права змінювати ідентифікатор безпеки.

11.4 Повинен бути заборонений будь-який безпосередній доступ до прикладного ПЗ і локальних баз даних функціональних задач ЦСК будь-якого користувача або груп користувачів, які є зовнішніми відносно ЦСК.

11.5 Перед отриманням доступу до РС, серверів або комунікаційного обладнання кожний користувач повинен ідентифікувати себе, вводячи ідентифікаційне ім'я входу в систему і пароль. Система повинна використовувати цю унікальну ідентифікацію для контролю дій користувача.

11.6 Для кожного користувача або групи користувачів повинні бути встановлені робочі станції ЦСК з яких він(вони) мають право виконувати вхід в систему.

11.7 Після здійснення успішного входу користувача в систему, повинен створюватися відповідний об'єкт-користувач, який уособлює користувача при будь-якому зверненні до ресурсів системи.

11.8 Об'єкт-користувач повинен бути пов'язаний з кожним об'єктом-процесом, який запускається користувачем.

11.9 Інформація, яка міститься в об'єкті-користувачі, повинна впливати на всі дії користувача або на будь-які процеси, які виконуються користувачем.

11.10 Всі об'єкти РС та серверів ЦСК повинні містити атрибути доступу в дескрипторі об'єкту.

11.11 Доступ користувача (об'єкту-процесу) до об'єкту повинен дозволятися за результатами порівняння атрибутів доступу об'єкта-користувача (об'єкта-процеса) з атрибутами доступу в дескрипторі об'єкту.

11.12 В системі захисту інформації ОС ЦСК повинна бути передбачений можливість створення облікових записів та збереження відомостей, необхідних для управління доступом до ресурсів системи. В системі повинні бути передбачені облікові записи користувачів та груп користувачів.

11.13 Кожний користувач, який працює в ЦСК, повинен мати локальний обліковий запис. Локальний обліковий запис повинен містити відомості про користувача і розміщуватися в локальній базі облікових записів безпеки конкретного комп'ютера.

11.14 Облікові записи для всіх користувачів повинні створюватися, модифікуватися і знищуватися тільки адміністратором безпеки ЦСК.

11.15 Об'єктами захисту є програмно-інформаційні ресурси ПТК ЦСК, в яких знаходиться, або може знаходитися інформація, яка підлягає захисту, а також програмне забезпечення, що реалізує технології оброблення такої інформації, для виконання ПТК ЦСК своїх функцій. До програмно-інформаційних ресурсів ПТК ЦСК, що підлягають захисту, відноситься сукупність даних певної логічної структури (файл, база даних), які циркулюють в ЦСК або окремих його компонентах. Відповідно до функціонального призначення, місця розміщення та виду представлення програмно-інформаційні ресурси наведені в табл. 11.1.

За рівнем повноважень щодо доступу до технічних та програмних засобів, інформації, що циркулює та накопичується в ПТК ЦСК, характером та змістом робіт, які виконуються в процесі функціонування, суб'єкти доступу поділяються на групи, які наведені в табл. 11.2.

Таблиця 11.1 - Програмно-інформаційні ресурси ПТК ЦСК, які є об'єктами захисту

{Д_ВЕБ}	Загальнодоступна інформація веб-сторінки
{Д_ЖУРr}	Журнали аудиту, що ведуться КЗЗ РС генерації ключів
{Д_ЖУРо}	Журнали аудиту, що ведуться КЗЗ РМ обслуговуючого персоналу
{Д_ЖУРС}	Журнали аудиту, що ведуться КЗЗ ЛОМ серверів ЦСК
{Д_ЗКСС}	Запит на керування статусом сертифіката
{Д_ЗКФС}	Запит на формування сертифікату
{Д_ЗМЧ}	Запит на мітку часу
{Д_ЗСС}	Запит статусу сертифіката
{Д_КФА}	Ключова фраза автентифікації, яка може бути використана підписувачем для подання запиту на блокування/скасування свого сертифікату (по телефону)

{Д_МЧ}	Мітка часу
{Д_ОКк}	Особисті ключі заявників, що генеруються на РС генерації ключів
{Д_ОКП}	Особисті ключі персоналу ІТС ЦСК
{Д_ОКЦ}	Особисті ключі ЦСК та серверів ЦСК
{Д_РП}	Реєстр підписувачів
{Д_СЕР}	Сертифікати ЦСК, серверів ЦСК, персоналу ЦСК та користувачів, списки відкликаних сертифікатів
{Д_СС}	Статус сертифіката
{Д_ТІКг}	Технологічна інформація КЗЗ РС генерації ключів
{Д_ТІКо}	Технологічна інформація КЗЗ РМ обслуговуючого персоналу
{Д_ТІКс}	Технологічна інформація КЗЗ ЛОМ серверів ЦСК
{Д_ТІУг}	Технологічна інформація управління РС генерації ключів
{Д_ТІУо}	Технологічна інформація управління РМ обслуговуючого персоналу
{Д_ТІУс}	Технологічна інформація управління компонентами ЛОМ серверів ЦСК

Таблиця 11.2 - Суб'єкти доступу до ресурсів ПТК ЦСК

Р_АР	Адміністратор реєстрації ЦСК
Р_АРЧЗ	Адміністратори реєстрації (чергова зміна)
Р_АЦ	Адміністратор сертифікації
Р_ЗПП	Користувачі ЦСК
Р_ЗАН	Анонімні користувачі ЦСК
Р_АБ	Адміністратор безпеки
Р_АС	Системний адміністратор
Р_ЗЗЯ	Заявники

11.16 Для користувачів ЦСК за виключенням Р_ЗПП, Р_ЗАН атрибутами доступу є реєстраційний запис користувача. Для користувачів Р_АБ, Р_АС атрибутами доступу є надане йому в системі ім'я облікового запису, пароль та мережева адреса. Для користувачів Р_ЗАН атрибутами доступу є лише його мережева адреса.

11.17 Для процесів, що функціонують на обладнанні ПТК ЦСК, атрибутами доступу є:

- списки персональних ідентифікаторів користувачів, що можуть отримати доступ до відповідного процесу;
- тип доступу (читання, модифікація, створення, видалення об'єкта) для кожного із компонентів списку.

11.18 Для інформаційних ресурсів ПТК ЦСК атрибутами доступу є:

- списки персональних ідентифікаторів користувачів, що можуть отримати доступ до кожного інформаційного ресурсу;
- тип доступу (читання, модифікація, створення, видалення об'єкта) для кожного із компонентів списку.

11.19 Взаємодія суб'єктів доступу і об'єктів захисту в ПТК ЦСК здійснюється згідно з адміністративним принципом керування доступом. Тільки адміністратор безпеки має право здійснювати реєстрацію об'єктів, що підлягають захисту, призначати користувачам повноваження та права доступу. Загальні правила розмежування доступу користувачів до ресурсів визначаються наступним чином згідно з табл. 11.3.

Таблиця 11.3 - Загальні правила розмежування доступу користувачів до ресурсів

№	Позначення	Право доступу			
		Читання	Створення	Модифікація	Видалення ¹
1	{Д_ТІКс}	Р_АБ	Р_АБ	Р_АБ	Р_АБ
2	{Д_ТІКо}	Р_АБ	Р_АБ	Р_АБ	Р_АБ
3	{Д_ТІКв}	Р_ВЗІ	Р_ВЗІ	Р_ВЗІ	Р_ВЗІ
4	{Д_ТІКг}	Р_АБ	Р_АБ	Р_АБ	Р_АБ
5	{Д_ТІУс}	Р_АБ, Р_АС	Р_АБ, Р_АС	Р_АБ, Р_АС	Р_АБ, Р_АС
6	{Д_ТІУо}	Р_АБ, Р_АС	Р_АБ, Р_АС	Р_АБ, Р_АС	Р_АБ, Р_АС
7	{Д_ТІУг}	Р_АБ, Р_АС	Р_АБ, Р_АС	Р_АБ, Р_АС	Р_АБ, Р_АС
8	{Д_ЖУРс}	Р_АБ, Р_АС	-	-	Р_АБ, Р_АС

¹ Під правом "видалення" для {Д_ЖУРс}, {Д_ЖУРо}, {Д_ЖУРв}, {Д_ЖУРг} мається на увазі їх повне очищення

№	Позначення	Право доступу			
		Читання	Створення	Модифікація	Видалення ¹
9	{Д_ЖУРо}	P_AB, P_AC	-	-	P_AB, P_AC
10	{Д_ЖУРr}	P_AB, P_AC	-	-	P_AB, P_AC
11	{Д_ОКП} ²	P_AЦ, P_AP, P_APЧЗ	P_AЦ, P_AP, P_APЧЗ	-	P_AЦ, P_AP, P_APЧЗ
12	{Д_ОКЦ}	P_AЦ ³	P_AB, P_AЦ ⁴	-	P_AB
13	{Д_ОКк}	P_ЗЗЯ	P_ЗЗЯ	-	-
14	{Д_КФА}	P_AP, P_APЧЗ	P_AP	P_AP	P_AP, P
15	{Д_РП}	P_AЦ, P_AP, P_APЧЗ	P_AP	P_AP	P_AP
16	{Д_СЕР}	УСІ	P_AЦ	-	P_AP, P_AЦ
17	{Д_ВЕБ}	P_ЗАН, P_AЦ	P_AЦ	P_AЦ	P_AЦ
18	{Д_ЗМЧ}	-	P_ЗАН	-	-
19	{Д_МЧ}	P_AB, P_AC	-	-	-
20	{Д_ЗСС}	-	P_ЗАН	-	-
21	{Д_СС}	P_ЗАН	-	-	-
22	{Д_ЗКСС}	P_AB, P_AC	P_AP, P_APЧЗ, P_ЗЗЯ	-	-
23	{Д_ЗКФС}	P_AB, P_AC	P_AP, P_ЗЗЯ	-	-

11.20 Спеціалісти, які здійснюють розробку та супроводження ПЗ, можуть отримати на момент проведення необхідних робіт будь-які ролі та права доступу, виконання яких здійснюється під контролем відповідного адміністратора.

11.21 Технічний обслуговуючий персонал може отримати доступ тільки до інформаційних об'єктів, що містять технічну, проектну, експлуатаційну документацію, до відповідних технічних засобів та необхідного для проведення робіт з їх обслуговування ПЗ.

11.22 Спеціалісти, які здійснюють розробку та супроводження ПЗ, заміну або модернізацію апаратних засобів ПТК ЦСК отримують доступ лише на момент проведення необхідних робіт і під контролем відповідного адміністратора.

11.23 Надання користувачу певної ролі, атрибутів доступу до певного ресурсу та його прав по доступу здійснюється тільки у випадках виконання таких умов:

- категорія користувача відповідає типу об'єкта захисту як це визначено в загальних правилах розмежування доступу (табл. 11.3);
- доступ до даного об'єкта захисту визначено службовими обов'язками користувача;
- вид взаємодії користувача з об'єктом захисту (перелік дій над об'єктом) встановлено специфікаціями послуг безпеки як дозволений (табл. 11.4);
- вид взаємодії користувача з об'єктом захисту (тип доступу) визначено службовими обов'язками користувача.

² Кожен користувач має права доступу тільки до власного особистого ключа

³ Під правом "читання" мається на увазі право на ініціювання процесу з використання особистого ключа відповідним засобом КЗІ

⁴ Процедура генерації {Д_ОКЦ} здійснюється спільними зусиллями користувачів з ролями P_AB та P_AЦ

12 ПРАВИЛА АДМІНІСТРУВАННЯ КЗЗ І РЕЄСТРАЦІЇ ДІЙ КОРИСТУВАЧІВ

12.1 Адміністрування облікових записів

Перед створенням (модифікацією) облікових записів користувачів адміністратор безпеки ЦСК повинен сформулювати вимоги до користувачів функціональних РС та серверів у вигляді облікової стратегії. При формуванні стратегії облікових записів користувачів адміністратор безпеки ЦСК повинен керуватися такими рекомендаціями:

1) до імен користувачів:

- облікові імена користувачів повинні бути унікальними;
- імена користувачів можуть містити до 20 будь-яких символів, окрім службових, на верхньому або нижньому регістрах;

2) до паролів користувачів:

- пароль повинен містити не менше 8 символів;
- користувач не має права змінювати пароль, призначений адміністратором безпеки;
- термін дії пароля для облікового запису кожного користувача повинен встановлюватися не більше 45 днів;
- для захисту від повторного використання можуть зберігатися не менше певного числа паролів, використаних раніше;
- паролі повинні бути конфіденційними і видаватися користувачам під розписку;
- списки нових паролів перед введенням в дію адміністратором безпеки повинні бути затверджені встановленим порядком;

3) до обмежень на робочі місця:

- робота користувача дозволяється тільки з власного функціонального АРМ.

Після планування і затвердження в установленому порядку облікова стратегія (політика) повинна бути основою для безпосередньої роботи з обліковими записами користувачів.

12.2 Адміністрування профілю користувача

Для кожної функціональної групи користувачів, які працюють на одному АРМ, повинна встановлюватися єдина системна політика послуги для груп, яка може автоматично завантажуватися при установці системи. Всі файли групової системної політики для всіх АРМ повинні бути заздалегідь підготовлені адміністратором безпеки ЦСК і розташовуватися на РС адміністратора безпеки.

Для будь-якого АРМ адміністратором безпеки повинен бути створений окремий обов'язковий єдиний профіль для всіх груп користувачів, які працюють на даному АРМ. При настройці обов'язкового профілю для кожної робочої станції адміністратор безпеки повинен в обов'язковому порядку заборонити загальний доступ до адміністративного інструментарію.

12.3 Адміністрування груп

Перед створенням (модифікацією) груп користувачів адміністратор безпеки ЦСК повинен розробити план створення локальних груп. При формуванні плану створення груп адміністратору безпеки доцільно керуватися наступними параметрами щодо визначення членства користувачів в групі:

- приналежністю до структурного функціонального підрозділу;
- виконуваними посадовими обов'язками;
- складом і варіантом функціональних задач на конкретній РС чи сервері;
- функціями, які виконуються при рішенні, як окремої задачі, так і всієї сукупності задач;

12.4 Адміністрування загальних ресурсів

Перед зміною (призначенням, видаленням, додаванням) прав доступу користувачів (груп) адміністратор безпеки ЦСК повинен виконати планування загальних ресурсів (загальних папок), керуючись такими рекомендаціями:

- скласти ієрархічну структуру ресурсів (додатків, даних, каталогів і т.п.) і визначити, які з них повинні бути загальними;
- ресурси з єдиними вимогами до захисту повинні розташовуватися на одному ієрархічному рівні;
- виділити групи, яким необхідний доступ до загальних ресурсів, і визначити типи доступу;
- для кожного загального ресурсу створити на відповідному комп'ютері локальну групу;
- права доступу до загального ресурсу повинні надаватися тільки тим групам, які дійсно вимагають доступу;
- вибрати максимально можливі права доступу;

- для забезпечення максимального рівня захисту повинні бути виключені права доступу на повний контроль групам “всі”, “користувачі”, “гості”;
- Необхідно оформити свої рішення у вигляді плану створення загальних ресурсів.

12.5 Адміністрування аудиту

Реєстрація всіх пов'язаних з безпекою подій в ЦСК повинна здійснюватися службою аудиту ОС. Аудит повинен реалізовуватися на тому технічному засобі, події якого необхідно відстежувати. Правила аудиту, що встановлені на РС або серверах, повинні розповсюджуватися тільки на ці РС (сервери). Контрольовані події повинні заноситися в локальний журнал безпеки. Адміністратор безпеки ЦСК може переглянути журнал або локально, або з РС адміністратора безпеки. В системі повинен забезпечуватися аудит як на рівні системних подій, так і на об'єктному рівні. Типи подій, які повинні реєструватися і протоколюватися в системі, повинні визначатися настройкою системи аудиту. Налаштування правил аудиту дозволяється тільки адміністратору безпеки ЦСК. Для забезпечення високого рівня захисту в системі повинні відстежуватися:

- невдалі і успішні спроби реєстрації користувачів;
- успішне і невдале використання будь-яких ресурсів;
- невдалі і успішні спроби зміни стратегії безпеки і адміністративної політики.

13 ЗАГАЛЬНІ ПРАВИЛА ВИКОРИСТОВУВАННЯ КРИПТОГРАФІЧНИХ ЗАСОБІВ

13.1 Використання криптографічних методів і засобів в обов'язковому порядку здійснюється на основі і з урахуванням керівних документів Адміністрації Держспецзв'язку України.

13.2 Для реалізації послуг конфіденційності, цілісності, автентифікації, управління доступом застосовуються криптографічні засоби захисту інформації на основі симетричної та асиметричної криптографії.

13.3 При роботі з ключовими документами повинні дотримуватися адміністративно-організаційні вимоги, обумовлені керівними документами Адміністрації Держспецзв'язку України.

13.4 Всі операції, які виконуються криптографічними засобами, і дії над ключами підлягають обов'язковому контролю і реєстрації в спеціальних журналах. Управління ключами здійснюється ПТК із складу ЦСК. Під управлінням ключами розуміються дії, пов'язані з генерацією, розподілом, доставкою, введенням в дію, зміною, збереженням, обліком, а також знищенням ключових даних і носіїв ключових даних.

13.5 В ЦСК можливо використання тільки сертифікованих або дозволених Адміністрацією Держспецзв'язку України до застосування засобів криптографічного захисту інформації.

13.6 Криптографічні засоби можуть бути реалізовані програмно, програмно-апаратний і апаратний. Найприйнятнішими для застосування є програмно-апаратні та апаратні засоби.

13.7 Всі криптографічні перетворення повинні виконуватися так, щоб виключалася можливість перехоплення або модифікації діючих ключів і паролів.

13.8 Всі випадки звернення до криптографічних засобів захисту інформації і результати виконання ними функцій повинні реєструватися в системі.

14 ПОРЯДОК ПРОВЕДЕННЯ РОБІТ ПО ЗАБЕЗПЕЧЕННЮ ФУНКЦІОНУВАННЯ

14.1 При роботі ЦСК використовується програмне забезпечення та технічні засоби різних виробників та різного призначення. Перелік програмного забезпечення та технічних засобів повинен бути наведений у паспорті-формулярі ЦСК із складу документації техноробочого проекту.

14.2 Засобами забезпечення відмовостійкості і захисту інформації в різній мірі оснащене все системне програмне забезпечення (операційні системи і мережні засоби). Прикладне програмне забезпечення також повинне бути оснащений засобами забезпечення відмовостійкості. Для детального ознайомлення з методами забезпечення відмовостійкості і захисту інформації, а також з порядком проведення робіт по відновленню і забезпеченню безперервності функціонування, необхідно керуватися документацією, яка поставляється разом з відповідним програмним забезпеченням.

14.3 Порядок проведення робіт по відновленню та забезпеченню безперервності функціонування ЦСК повинен бути визначений у відповідному плані проведення відновлювальних робіт і забезпечення неперервного функціонування ЦСК.

15 ВІДПОВІДАЛЬНІСТЬ ЗА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В ЦСК

15.1 Служба захисту інформації в ЦСК і керівники більш високого рівня відповідають за:

- проведення ефективного управління ризиком (ідентифікацію цінностей, які підлягають захисту, визначення вразливих ресурсів, аналізу ризику, їх використання і реалізації рентабельних засобів захисту);
- визначення і формування ефективної політики безпеки;
- своєчасне інформування співробітників щодо цієї політики;
- здійснення програми навчання основам безпеки для користувачів, яка гарантує знання ними діючих політик безпеки і правил роботи;
- гарантію того, що весь персонал ЦСК знає політику безпеки інформації, прийняту на даному рівні;
- своєчасне інформування адміністраторів безпеки і системних адміністраторів про зміни в статусі будь-якого користувача ЦСК.

15.2 Адміністратори безпеки ЦСК відповідають за:

- впровадження і реалізацію затвердженої політики безпеки, оперативне управління і підтримку реалізованих заходів захисту;
- коректне застосування доступних механізмів захисту для реалізації часткових політик безпеки;
- інформування керівництва про працездатність існуючих політик безпеки і підготовку технічних пропозицій, які могли б підвищити її ефективність;
- захищеність середовища ЦСК і інтерфейсів з іншими підсистемами і зовнішніми мережами;
- виявлення і усунення порушень безпеки;
- використання доступних і надійних засобів аудиту для полегшення виявлення порушень безпеки;
- проведення своєчасних перевірок системних журналів і журналів обліку порушень безпеки;
- коректне застосування своїх прав і повноважень;
- розробку відповідних процедур та інструкцій щодо запобігання, виявлення і віддалення несанкціонованого (зловмисного) програмного забезпечення;
- своєчасне створіння резервних копій всіх даних і програмного забезпечення;
- підтримку функціонування пакетів антивірусних програм;
- розробку процедур інформування користувачів про виявлені порушення безпеки;
- надання допомоги при визначенні джерела зловмисного програмного забезпечення, зони його розповсюдження і наступного віддалення.
- надання користувачам доступу до необхідних даних, програм, функцій і ресурсів мережі ЦСК;
- надання/відміну прав і повноважень, настройку робочих параметрів засобів захисту;
- контроль за всіма пов'язаними із захистом подіями і за розслідуванням будь-яких реальних або підозрюваних порушень;
- оперативне припинення порушень безпеки, які виникають в окремих компонентах ЦСК в процесі функціонування ЦСК;
- підтримку і захист програмного забезпечення і відповідних файлів на серверах і робочих станціях ЦСК, використовуючи доступні механізми і процедури захисту;
- регулярну перевірку серверів і робочих станцій ЦСК за допомогою запуску антивірусного програмного забезпечення;
- присвоєння ідентифікаційних атрибутів кожному користувачу;
- своєчасне інформування керівництва про всі порушення безпеки інформації.

15.3 Користувачі ЦСК відповідають за:

- розуміння і дотримання відповідних законодавчих актів України, нормативних документів, політик безпеки і пов'язаних з ними процедур, прийнятих в ЦСК;
- правильне використання доступних механізмів безпеки для захисту критичної інформації і ресурсів ЦСК;
- правильне використання апаратно-програмних компонентів ЦСК в цілому відповідно до діючої політики безпеки;
- допомога іншим користувачам у використанні механізмів захисту належним чином, в захисті ресурсів іншим користувачам, інформування про незахищеність їх ресурсів;
- своєчасне інформування адміністраторів безпеки про будь-яку підозру на порушення захисту;

- знання і використання відповідних політик і процедур для запобігання, виявлення і віддалення зловмисного програмного забезпечення;
- знання і правильне виконання процедур щодо забезпечення безперервної роботи і відновлення при потенційних інцидентах.

15.4 Особи, винні в порушенні порядку і правил захисту оброблюваної в ЦСК інформації, несуть дисциплінарну, адміністративну, кримінальну або матеріальну відповідальність відповідно до чинного законодавства України.

16 ПОРЯДОК РОЗРОБКИ І СУПРОВОДУ КСЗІ

16.1 Згідно ДСТУ 3396.0-96 і ДСТУ 3396.1-96 забезпечення безпеки інформації в ЦСК здійснюється поетапно.

1 етап – визначення і аналіз загроз;

2 етап – розробка системи захисту інформації;

3 етап – реалізація плану захисту інформації;

4 етап – контроль функціонування і управління системою захисту інформації.

16.2 На першому етапі здійснюється обстеження об'єктів інформаційної діяльності (об'єктів ЕОТ). В процесі обстеження необхідно здійснити аналіз об'єктів захисту (ідентифікацію цінностей), ситуаційного плану і умов функціонування ЦСК, аналіз загроз і їх наслідків (оцінка ризиків), визначення слабкості в захисті. Загрози повинні бути визначені в термінах вірогідності їх реалізації і величини можливого збитку. Ризик є функцією вірогідності реалізації певної загрози, вигляду і величини заподіяного збитку. Оцінка ризику здійснюється на підставі аналізу загроз, існуючих в системі вразливостей, ефективності вже реалізованих заходів захисту ресурсів ЦСК. Величина ризику може бути визначена в грошовому вимірі або у вигляді формальної оцінки (високий, низький і т.п.). За наслідками обстеження складається акт, здійснюється категоріювання об'єктів ЕОТ, розробляється модель загроз інформації в ЦСК і формується політика безпеки інформації.

16.3 На другому етапі, на підставі проведеного аналізу ризиків і сформульованої політики безпеки, здійснюється вибір функціонального профілю захищеності ЦСК від несанкціонованого доступу і вимоги до захищеності інформації від витоку технічними каналами. Функціональний профіль захищеності інформації в ЦСК визначається відповідно НД ТЗІ 2.5-005-99 на підставі класу АС. Вимоги до захищеності інформації від витоку технічними каналами визначаються на підставі Правил посиленої сертифікації.

Для реалізації функціонального профілю захищеності ЦСК здійснюється вибір ефективних і економічних захисних заходів і механізмів і розробляється план захисту інформації в ЦСК, який визначає послідовність і зміст етапів робіт по впровадженню і експлуатації КСЗІ. В доповненні до комплексу програмно-технічних способів захисту інформації визначаються організаційні, фізичні і інші заходи захисту, які реалізуються поза обчислювальною системою ЦСК. До складу КСЗІ повинні включатися захисні заходи і механізми, реалізація яких дозволила б понизити рівень остаточного ризику до допустимого рівня. Вартість заходів щодо захисту інформації в ЦСК повинна бути адекватна величині можливого збитку.

16.4 Третій етап робіт по забезпеченню безпеки інформації в ЦСК полягає в реалізації плану захисту інформації. В процесі виконання робіт здійснюється реалізація і перевірка вибраних заходів і механізмів захисту. За наслідками реалізації заходів захисту інформації слід скласти в довільній формі акт приймання робіт, який повинен бути підписаний виробником робіт, погоджений з начальником служби захисту інформації (СЗІ) ЦСК і затверджений керівництвом ЦСК.

16.5 Четвертий етап – контроль функціонування і управління КСЗІ - реалізується на стадії експлуатації ЦСК і полягає в аналізі функціонування КСЗІ з метою оцінки її ефективності і розробки додаткових (уточнюючих) вимог для доробки при зміні початкових умов (характеристик обчислювальної системи, оброблюваної інформації, фізичного середовища, персоналу, призначення ЦСК, політики безпеки і т.п.). Процес управління КСЗІ (управління ризиками) повинен підтримуватися протягом всього життєвого циклу ЦСК.

16.6 Реалізація функцій і задач КСЗІ ЦСК повинна забезпечуватися комплексним використанням методів і засобів криптографічного і технічного захисту інформації.

17 ПОРЯДОК РЕАГУВАННЯ НА ПОРУШЕННЯ БЕЗПЕКИ

17.1 При порушенні встановлених політикою правил безпеки інформації (порушення конфіденційності, доступності, спостереженості, цілісності даних, інформаційних ресурсів) необхідно:

- негайно зупинити процес, в ході якого встановлено порушення безпеки (обробка, передача інформації і т.п.);
- блокувати програмно-апаратні засоби доступу в систему;
- в ручному або автоматичному режимі доповісти про факт порушення адміністратору безпеки і керівнику функціонального підрозділу, де мав місце факт порушення.

17.2 За фактом порушення безпеки повинне проводитися адміністративне розслідування комісією, яка призначається керівником ЦСК. Результати розслідування оформляються актом за підписами членів комісії. Акт затверджує керівник ЦСК, який письмово або в усній формі дає розпорядження керівнику функціонального підрозділу про усунення виявлених недоліків або порушень безпеки.

17.3 Керівник функціонального підрозділу, в якому мало місце порушення безпеки, відповідно до розпорядження керівника ЦСК розробляє порядок, терміни і заходи щодо усунення виявлених недоліків або порушень безпеки.

17.4 Залежно від характеру порушень (навмисні або випадкові), їх ваги (нанесеного збитку) приймаються відповідні заходи реагування. До осіб, які винні в порушенні безпеки, повинні застосовуватися заходи дисциплінарної, адміністративної, кримінальної або матеріальної відповідальності відповідно до чинного законодавства України. Відповідальність за порушення безпеки користувачами ЦСК і застосування відповідних заходів дії повинні бути регламентовані окремими положеннями, затвердженими за встановленим порядком.

18 ОРГАНІЗАЦІЯ НАВЧАННЯ І ПЕРЕПІДГОТОВКИ ПЕРСОНАЛУ

18.1 Затверджена політика безпеки в ЦСК, а також способи і засоби захисту, повинні доводитися до відома всіх користувачів і персоналу ЦСК з використанням різних форм навчання (наприклад, лекції, семінари, інструктажі, самостійна робота згідно завдань керівників функціональних підрозділів, які погоджені з службою захисту інформації в ЦСК, практичні заняття і т.п.).

18.2 Поглиблене навчання і перепідготовка персоналу і користувачів повинне проводитися на:

- курсах, які створюються ДП "ЕНЕРГОРИНОК" спільно з підприємствами-розробниками прикладного програмного забезпечення і апаратно-програмних засобів захисту;
- базах кафедр вищих навчальних закладів, які здійснюють підготовку фахівців в області безпеки інформації.

Персонал і користувачі по завершенню різних форм навчання і перепідготовки повинні одержувати відповідні свідоцтва.